values. For example, the algebraic equation for the valid program detection routines can include an equation as given by:

$$\text{VALID SCORE} = \sum_{i=1}^{M} W_i,$$

[0042] where W_i=weight of a valid detection routine v_i for i=1 to M.

[0043] Similarly, the algebraic equation for the malicious code detection routines can include an equation as given by:

$$\text{MALICIOUS CODE SCORE} = \sum_{j=1}^{N} W_j,$$

[0044] where W_j=weight of a malicious code detection routine t_j for j=1 to N.

[0045] In another embodiment, more complex forms of the scoring algorithm **44** can be implemented in the form of more sophisticated algebraic formulae.

[0046] If a program under investigation exceeds a valid program score threshold, V_{thres}, then it is determined that the program is a valid program. If that program exceeds a malicious code score threshold, T_{thres}, then it is determined that the program is a malicious code program. If a program is deemed to be valid using the valid algorithm, then it is sometimes eliminated from consideration as a malicious code program.

[0047] Executable code and/or programs under investigation may also have some of the characteristics and behaviors of valid programs and some of the characteristics and behaviors of malicious code. If a program does not exceed either threshold or if a program does not have a significant difference between the valid program score **56** and the malicious code score **58**, then according to another embodiment of the present disclosure, the technique identifies the program in another category of suspicious programs or anomalous programs.

[0048] In one embodiment, the technique for detecting malicious code on a computer system includes executing a malicious code detection program on the computer system. The malicious code detection program includes detection routines. The malicious code detection program applies the detection routines to programs on the computer system. The detection routines are assigned weights that are factored by a scoring algorithm to determine a composite score based on the results of the detection routines and their associated weights. For example, a malicious code detection routine has a weight associated with it, such that if the malicious code detection routine determines that a given code under investigation is a malicious code program, then the weight is applied positively towards the malicious code score for the code under investigation. Also, the malicious code detection program determines whether one or more programs are valid or malicious as a function of the weights assigned to the detection routines.

[0049] In another embodiment, the technique is configured to detect malicious code on a computer having an operating system. The technique includes executing a malicious code detection program on the computer. Detection routines of the malicious code detection program are configured to gather information about programs on the computer system. The detection routines include at least one selected from the group consisting of (a) examining each executable code or program itself and (b)searching for information about each executable code or program in the operating system. For example, examining code or a program can include examining a binary image of the same, wherever the binary image may reside, within the IHS or in computer readable media accessible to the IHS. In addition, the detection routines further consist of valid program detection routines and malicious code detection routines.

[0050] The malicious code detection program applies the detection routines to the programs on the computer system. In response to a detection of a valid program or malicious code, the detection routines assigns weights to respective programs under test as a function of a respective detection routine. Also, the malicious code detection program determines whether a program is a valid program or malicious code as a function of the weights assigned by the detection routines. Determining whether the program is a valid program or malicious code involves the scoring of an execution of each detection routine as a function of a respective weight. A scoring algorithm is used to identify a program as malicious code in response to a valid score and a malicious code score, as discussed herein.

[0051] In yet another embodiment, the technique for detecting malicious code on a computer system includes executing detection routines, the detection routines having been configured to examine at least one selected from the group consisting of characteristics and behaviors of programs on the computer system. For example, the detection routines can be configured to access process behavior information of a program on the computer system. In addition, the characteristics and behaviors may include one or more of logging keystrokes, saving a display screen view, uploading files, downloading files, executing programs, and controlling a display screen of the computer system.

[0052] Subsequent to execution of one or more of the detection routine, weights are assigned as a function of the examined characteristics and behaviors, the assigned weights indicative of a valid program or malicious code as a function of respective detection routines. Also, the technique determines whether a program is malicious code as a function of the weights assigned by the detection routines.

[0053] In the embodiment of the previous paragraph, the detection routines include valid program detection routines and malicious code detection routines. The valid program detection routines are configured to determine whether the program exhibits at least one or more characteristics and behaviors associated with a valid program. The malicious code detection routines are configured to determine whether the program exhibits at least one or more characteristics and behaviors associated with malicious code.

[0054] In one embodiment, the technique for detecting malicious code is implemented in the form of a computer program. The computer program is executed on a desired computer system for detecting any potential malicious code